Army Cyber Mission Force – Ambitions and Realities

A Monograph

by

COL Kevin P. Romano
U.S. Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2015

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-17-2015	SAMS Monograph	

4. TITLE AND SUBTITLE

Army Cyber Mission Force – Ambitions and Realities

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

COL Kevin P. Romano

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
KS 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Advanced Strategic Leadership Studies Program

10. SPONSOR/MONITOR'S ACRONYM(S)

CGSC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The 2010 US Army Training and Doctrine Command's Concept Capability Plan for Cyberspace Operations directed the Army to begin development of a Cyber Mission Force. The direction to build a Cyber Mission Force followed a number of cyberspace attacks conducted to support military operations. The foundation of the Cyber Mission Force will be the highly technical soldiers are trained to operate in the cyberspace domain. To develop this force the Army will need to adequately recruit, retain, and organize for success. The study found that the Army's current approach to recruiting, retaining, and organizing a Cyber Mission Force will not meet the goals of the Army. The findings suggest that Army must readdress branding, compensation, professional development and organization in order to increase the likelihood of success for the Cyber Mission Force.

15. SUBJECT TERMS

Allied Powers, Axis Powers, Coalition, Dieppe, Raid, Second World War, Canada, United States, Britain, Russia

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
Unclassified	Unclassified	Unclassified		48	913-758-3302

Monograph Approval Page

Name of Candidate: COL Kevin P. Romano

Monograph Title: Army Cyber Mission Force – Ambitions and Realities

Approved by:

_____, Monograph Director
William J. Gregor, PhD

_____, Seminar Leader
Robert W. Tomlinson, PhD

_____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL, IN

Accepted this 23nd day of May 2015 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Abstract

Army Cyber Mission Force – Ambitions and Realities, by COL Kevin P. Romano, Army, 48 pages.

The 2010 US Army Training and Doctrine Command's Concept Capability Plan for Cyberspace Operations directed the Army to begin development of a Cyber Mission Force. The direction to build a Cyber Mission Force followed a number of cyberspace attacks conducted to support military operations. The foundation of the Cyber Mission Force will be the highly technical soldiers trained to operate in the cyberspace domain. To develop this force the Army will need to recruit, retain, and organize for success. Research has shown that persons drawn to highly technical fields, such as cyberspace, possess unique character traits that differ from the typical traits of Army enlistees. The research has further shown that compensation, branding, professional development models, and organization are key factors in the recruitment and retention of cyberspace professionals in both the military services and private sector.

Assessing the Army's model for recruiting, retaining, and organizing a Cyber Mission Force required a number of steps. First, it was necessary to understand the unique generational and character traits for those drawn to highly technical fields. The next step involved comparing Air Force and private sector branding with that of the Army. The research also examined compensation differences between the Air Force, private sector, and the Army in regard to recruiting and retaining cyberspace professionals. Next followed analysis of professional development models for cyberspace professionals and how professional development directly impacts retention of cyberspace professionals. The last step involved examining how the Air Force, private sector and the Army approach organizing for cyberspace operations.

The study found that the Army's current approach to recruiting, retaining, and organizing a Cyber Mission Force is unlikely to meet the Army's goals. The findings suggest that Army must readdress branding, compensation, professional development and organization in order to increase the likelihood of success for the Cyber Mission Force.

Contents

Acronyms

ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
AFSC	Air Force Specialty Code
AMRG	Army Marketing Research Group
AR	Army Regulation
ARCYBER	U.S. Army Cyber Command
BEAR	Bonus Extension and Retraining Program
CEMA	Cyber Electromagnetic Activities
CF	Career Field
CMF	Career Management Field
CPB	Cyber Protection Brigade
CPT	Cyber Protection Team
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CO	Cyberspace Operations
CSRB	Critical Skills Retention Bonus
CyMF	Cyber Mission Force
DA	Department of the Army
DCO	Defensive Cyberspace Operations
DOD	Department of Defense
DODIN	Department Of Defense Information Networks
DSRB	Deployed Selective Reenlistment Bonus
ESRB	Enhanced Selective Reenlistment Bonus
FM	Field Manual
JAMRS	Joint Advertising and Marketing Research Studies

JP	Joint Publication
MOS	Military Occupation Specialty
NCOES	Noncommissioned Officer Education System
OCO	Offensive Cyberspace Operations
S&IP	Special and Incentive Pay
SRB	Selective Reenlistment Bonus
TRADOC	Training and Doctrine Command

Figures

Tables

Introduction

> "We are facing the threat of a new arena in warfare that could be every bit as destructive as 9/11 — the American people need to know that. We can't hide this from the American people any more than we should have hidden the terrorism-attack threat from the American people."
>
> —Former Secretary of Defense Leon Panetta[1]

Over the past forty five years the Department of Defense's Advanced Research Projects Agency (ARPA) has revolutionized the world in unimaginable ways. In December 1969, the Advanced Research Projects Network (ARPANET) successfully linked together computers from the University of Utah, University of California, Santa Barbara; University of California, Los Angeles; and Stanford University. Over the next 40 years the four node ARPANET evolved to become what we now know as cyberspace. Cyberspace is now a recognized domain analogous to land, sea, air, and space.

In light of maturing Internet and networking technologies in the late 20th century more and more military planners increasingly look to cyberspace as a new domain for operations. Cyberspace materialized in the former Soviet Republic of Estonia on 27 April 2007. A bitter controversy surrounded the relocation of a Soviet era war memorial in Estonia. On the morning of April 27th, a series of coordinated cyberspace-based attacks targeted critical Estonian government and commercial entities. The targets included banks, newspapers, government ministries, and public broadcasters. The attack damaged the targets just as surely as a conventional attack with bombs or rockets. The events of 2007 were harbingers of things to come.

The summer of 2008 saw Russia embroiled in conflict with the former Soviet Republic of Georgia over the heavily ethnic Russian region of South Ossetia. In support of the military

---

[1] Mark Thompson, "Panetta Sounds Alarm on Cyber-War Threat," *Time*, October 12, 2012, 1, accessed July 14, 2014, http://nation.time.com/2012/10/12/panetta-sounds-alarm-on-cyber-war-threat/.

operation, in late July and early August, Russia deployed a coordinated series of cyberspace attacks aimed at crippling key Georgian government and private sector entities. The attacks represented the first documented incident in which cyberspace attacks were launched by a nation in direct support of combat operations. The Russian attacks, in the opinion of many analysts, greatly contributed to the favorable Russian outcome in the war. The events in Georgia clearly showed that cyberspace presented new opportunities and vulnerabilities for military operations.

The events in Estonia and Georgia, coupled with the rise of State and non-State actors in cyberspace caused military and government officials in the United States to assess their own capabilities. In particular, the United States Army undertook a thorough analysis of the vulnerability of the force to cyberspace threats. The year 2010 was a landmark year for the development of Army cyberspace capabilities. The major Army accomplishment was publication of Training and Doctrine Command (TRADOC) Pamphlet 525-7-8, *Cyberspace Operations Concept Capability Plan 2016-2028* in February 2010. The pamphlet codified the Army's goals for a cyberspace operations.

TRADOC Pam 525-7-8 clearly identified the need for a trained Cyber Mission Force. Army leaders also recognized that building an organic cyberspace force would be difficult in the face of competition for qualified personnel from other military services, governmental agencies and private sector businesses. The Army chose to establish a Cyber Mission Force (CyMF) to serve as the primary organization to achieve the Army's cyberspace goals. The CyMF seeks to accomplish several tasks deemed critical to providing an Army cyberspace capability. First, the CyMF provides the Army personnel needed to fulfill Service and Joint cyber requirements. Army specific requirements include, but are not limited to manning ARCYBER, 1st Information Operations Command, and the Network Enterprise Technology Command. Joint cyberspace requirements for the Army include supporting US Cyber Command, the National Security Agency, and the Defense Information Systems Agency. In the future CyMF personnel will fulfill

institutional training requirements for the Army and Joint force. However, the Army presently places priority on filling operational cyberspace positions. Secondly, the CyMF will provide the foundation for the Army's Cyber Protection Brigade (CPB) and its associated Cyber Protection Teams (CPT). The CPB structure represents the key Army organization explicitly designed to provide offensive and defensive cyberspace capabilities to the force.

There are three well-identified aspects to any recruitment and retention problem. First, there is the recruiting market. The market consists of the available population of recruits. That population consists of persons possessing the required skills, but not currently employed; those currently employed in the field; and those with the potential to acquire the needed skills. The market also includes all public and private enterprises who compete to hire and retain those persons. The second aspect is the enterprise's system for compensation and retention. Lastly, there is the enterprise's system for effectively and efficiently managing the force. By carefully describing the market and its participants and by identifying and comparing both Army and its competitor's practices, it was possible to make an assessment of the Army's likelihood of success.

However, to build the description of the market and the recruiting and retention practices across widely differing organizations it was important to first develop a common lexicon of key terms and concepts that would facilitate the research. This first step was necessary since the investigation would cross many different fields including: private sector human resource management, military personnel management, occupation categories, compensation, and technical training. This step of study required the identification and use of accepted terms and definitions commonly used in the private and government sectors. Based on rapid growth of careers in cyberspace a special effort was made to define what constitutes a cyberspace career. Second, it was necessary to address the question from three perspectives: the Army; its military service competitor, the Air Force, and a private enterprise, in this case the Sprint Corporation

(Sprint). The Air Force and Sprint were chosen because both have a long, successful history of organizing a cyberspace workforce. The method employed was to compare proven successful approaches used by the Air Force and Sprint Corporation against the proposed construct of the Army. The US Army Cyber Center of Excellence, the U.S. Air Force 81st Training Group, and Sprint Corporation each provided recruiting, retention, and organizational data. U.S. Government agencies and the RAND Corporation provided workforce supply and demand projections along with the unique generational and personality traits of the future cyberspace workforce.

The analysis of Army and competitor practices and the manpower market strongly suggests that despite Army aspirations, the U.S. Army will fail to meet its objectives in developing a Cyber Mission Force because its recruiting, retention, and organization are not suited for highly technical positions. Army recruiting is not designed to attract the best quality candidates into the Cyber Mission Force. Army retention strategies are not designed properly to retain those soldiers with highly technical, perishable skills like those inherent in the Cyber Mission Force. Army organization of its cyber capabilities is spread among several different and competing organizations that creates redundancies, inefficiencies, and internal competition.

Defining the Population

To create the common foundation upon which the findings of this research rests it was necessary to define a number of key terms. The terms that need a common lexicon are: recruiting, retention, entry level, and mid-career level. These terms required a common understanding based upon the requirement to adequately compare military and civilian structures. The Dictionary of Human Resources and Personnel Management defines recruiting as, "to search for and appoint new staff to join a company."[2] Similarly, retention is, "the process of keeping the loyalty of

[2] A Ivanovic, *Dictionary of Human Resources and Personnel Management*, 3rd ed.

existing employment and persuading them (employees) not to work for another company."[3] In a similar manner it was necessary to define entry and mid-career classification standards for the military based on the need to compare military and civilian career progression. The O*NET Dictionary of Occupational Titles based on U.S. Department of Labor rankings creates five job zones that define experience needed to perform a job. For this research entry level corresponds to Job Zone 3: "Medium preparation needed. Previous work related skill, knowledge or experience is required for these occupations."[4] For military personnel, this designation applies to E3-E5, WO1, and O1-O3 pay grades. In a similar light, mid-career is determined to correspond to Job Zone 4: "Considerable preparation needed. A minimum of 2-4 years of work related skill, knowledge, or experience is needed for these occupations."[5] The military grades corresponding to this classification include E6-E8, CW2-CW3, and O4-O5. The definitions provided above create the metric on which to compare military and private sector cyberspace careers.

Initially it might seem clear what individuals are employed in cyberspace careers. However, the term cyberspace as used by the military actually refers to a subset of what is generally called Information Technology. Using information from the U.S. Bureau of Labor Statistics, U.S. Department of Labor, and O*NET, it was determined that a cyberspace career is one that meets the following standard, "Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May

---

(London: A & C Black, 2006), 219.

[3] Ibid., 227.

[4] Susan Pines, Veda Dickerson, and Lori Cates, eds., *O*NET Dictionary of Occupational Titles*, 2nd ed. (Indianapolis: JIST Publishing, 2003), s.v. "Experience.", 15.

[5] Ibid.

respond to computer security breaches and viruses."[6] Military and private sector cyberspace professionals undergo similar training and perform similar duties. This commonality facilitated the comparison of military approaches and the private sector approaches.

Future Supply and Demand for Cyberspace Professionals

Private sector careers in cyberspace started initially in the early 1990s. Originally, these careers fell under the broader career category of Information Technology. Since the 1990s cyberspace careers have grown phenomenally. While demand for cyberspace professionals has spurred an increase in the supply, the supply of professional has, nevertheless, fallen well short of the demand. Data from the U.S. Bureau of Labor Statistics provides the following outlook:

[6] Ibid.

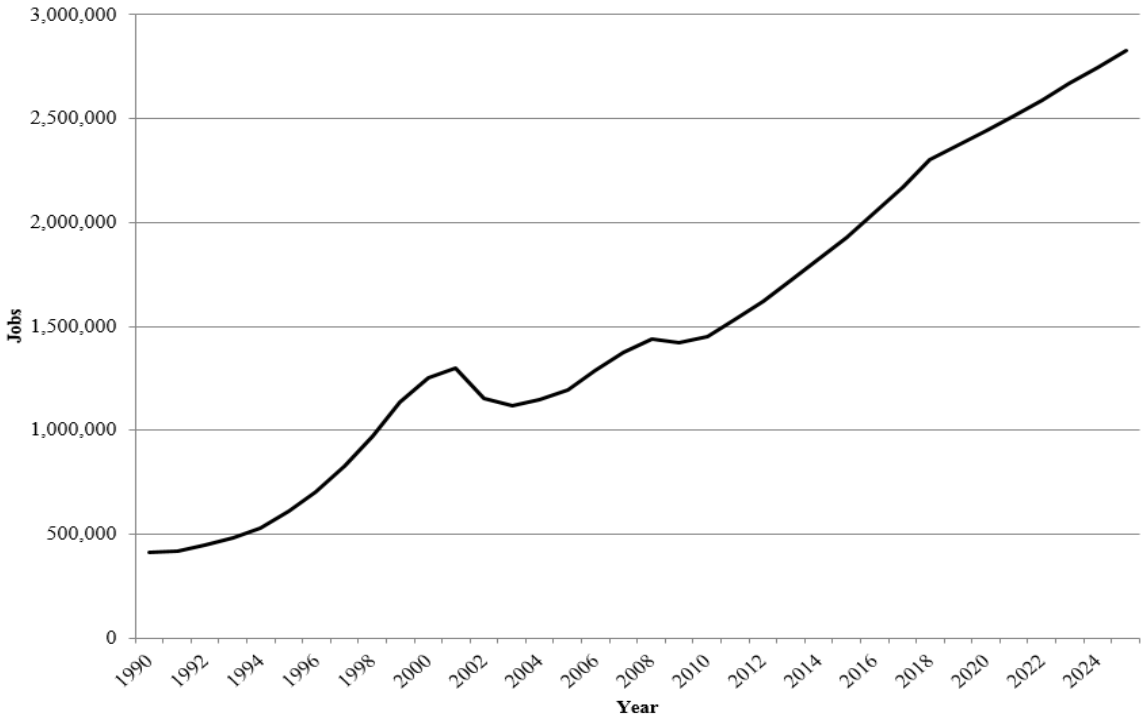

Figure 1. Growth of Cyberspace Careers[7]

Source: Lauren Csorny, "Careers in the Growing Field of Information Technology," US Bureau of Labor Statistics, April, 2013.

Jeff Moss, advisor to the Homeland Security Advisory Council sounded the alarm in 2012 when he stated, "None of the projections look positive. The numbers I've seen look like shortages in the 20,000s to 40,000s for years to come."[8] The US Bureau of Labor Statistics predicts that the demand for cyberspace/information security professionals will grow by 53%

[7] Lauren Csorny, "Careers in the Growing Field of Information Technology," U.S. Bureau of Labor Statistics, April, 2013, accessed November 10, 2014, http://www.bls.gov/opub/btn/volume-2/careers-in-growing-field-of-information-technology-services.htm.

[8] Jim Finckle and Noel Randewich, "Experts Warn of Shortage of U.S. Cyber Pros," Reuters, June 12, 2012, accessed August 14, 2014, http://www.reuters.com/article/2012/06/12/us-media-tech-summit-symantec-idUSBRE85B1E220120612.

between 2013 and 2018 and then grow another 37% between 2018 and 2022.[9] This represents one of the faster growing career fields tracked by the Bureau. The shortage of personnel to meet the demand in the public and private sectors coupled with increasing compensation will constrain development of cyberspace capabilities.

Recruiting Market

Two primary characteristics of the cyberspace professional population will make the competition for talent difficult, not only for the Army but also the private sector. The character factors are the generational differences and unique personality traits of those drawn to highly technical fields such as cyberspace. Previous research appearing in Army professional journals fell short in addressing the future soldiers needed by the Army to meets its growing cyberspace ambitions. Ground breaking work by Colonel Greg Conti[10] of the United States Military Academy, while influential at the time, focused solely on the Millennials.[11] Missing was the focus on *Force 2025 and Beyond*. The soldiers that will form the core of *Force 2025 and Beyond* are now known as Generation Z. Generation Z are those Americans born since 2000 and euphemistically known as "digital natives." The unique characteristics of Generation Z include[12]:

- Able to multi-task and process large amounts of data, but it must be broken into small pieces.
- 64% have constant Internet access.
- Spends 8-9 hours per day connected to at least one form of media.
- 90% of secondary students have mobile devices, 20% of elementary students.

[9] U.S. Bureau of Labor Statistics, "Information Security Analysts," U.S. Bureau of Labor Statistics, January 8, 2014, accessed August 14, 2014, http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[10] See recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture in July 2012 edition of *Small Wars Journal*.

[11] Millennials are those youth that reached adulthood, normally age 21, in the year 2000.

[12] Lishia Whitworth and Sara White, "Facts About Gen Z," Tech with Class, accessed August 20, 2014, http://techwithclass.webs.com/facts-about-gen-z.

- The most independent generation in recent history.
- Spend the least amount of time in human history using conversation to get ideas across - an “unreal” reality (virtual interaction).
- Are less healthy and generally more obese.
- Make rapid decisions; use very little time to contemplate consequences.
- 60.2% want to become an authority in their field.

Among the characteristics listed above, several require special emphasis when considering the CyMF. First, the inherent desire for independence will influence this generation not only in their personal but also their professional lives. This will have significant ramifications for how the Army effectively leads and manages these Soldiers. Second, an exceedingly high number of this generation want to become experts in their respective fields. This will likewise affect how this group will view advancement and career progression in the Army. Specifically, this generation will not view moving into leadership and management position as success. Not unique to the CyMF specifically, but this generation will enter the Army in poorer physical condition than any previous cohort. While poor physical conditioning can be overcome during initial training, it can, deter a person from considering the Army as a career choice. Finally, research indicates that Generation Z greatly values employment earning and compensation. The source of this trait many believe can be traced to the economic recession of 2008 when many Generation Z children saw their parents lose jobs and life savings almost overnight. Generational differences will not be an area that can be overlooked by any organization, public or private, looking to develop capabilities in cyberspace.

Businesses hold the perception that those drawn into highly technical fields such as cyberspace have unique personalities. To investigate and identify the unique traits of cyberspace professionals, Northrop Grumman Corporation along with Virginia-based Semper Secure conducted the landmark Cyber Security Census in 2013. The objective of the Cyber Security Census was to “determine what motivates today’s cyberspace professionals and how do we train

and recruit the next generation?"[13] Semper Secure surveyed over 500 cyberspace professionals from 40 different industries across 43 states including the District of Columbia and Puerto Rico. The research by Semper Secure, when applied to the CyMF problem, provides insight into how to recruit and retain cyberspace processionals.

The first question asked in the Cyber Security Census was what attributes a cyberspace professional considers most important when looking at a potential employer. Forty-four percent of the prospective workers answered that an employer must demonstrate a well-respected code of honor. Thirty-four percent wanted an employer who was a leader in cyberspace. Thirty-three percent wanted him to be a leader in addressing cyberspace.[14] A portion of the Cyber Security Census also examined issues related to recruitment. Researchers investigated two different demographic groups; those that changed to a cyberspace career and those whose only work experience was cyberspace. The top-three relative motivators for each group are found in the table below.

Table 1. Cyberspace Career Priorities[15]

Priority	Changed to Cyberspace Career	Only Cyberspace Career
1	Work of National Importance	Technology
2	Work Flexibility	Compensation
3	Technology	Control over work & environment

Source: Cyber Security Census (Mechanicsville, VA: Semper Secure, 2013), 3.

The implications are readily evident. Compensation and benefits are extremely important; as best stated by the Cyber Security Census, "make no mistake – money matters."[16] Candidly, for any

[13] Cyber Security Census (Mechanicsville, VA: Semper Secure, 2013), 3.

[14] Ibid., 14.

[15] Ibid., 19.

[16] Ibid., 14.

organization, government or private sector, to have the best cyberspace workforce you must be willing to pay for the best.

Recruiting the Best and Brightest

There are literally countless factors that either contribute or detract from an organization's recruiting efforts. Some that immediately come to mind include the brand or perception of the organization, compensation, opportunity for advancement, professional and personal fulfillment. The American Marketing Association (AMA) defines a brand as a "name, term, sign, symbol or design, or a combination of them intended to identify the goods and services of one seller or group of sellers and to differentiate them from those of other sellers."[17] For the purpose of this work the focus will be on organizational branding and compensation.

The US Air Force's development of cyberspace capabilities predates that of the other armed services, particularly the Army, by nearly a decade. The Air Force began to look at cyberspace shortly after 2000. What followed was a rapid development of doctrine, organization, training, and personnel structure to support the Air Force vision of operating in cyberspace. Air Force recruiting and retention strategies fell under the larger umbrella of personnel structure. The Air Force made a concerted effort to brand itself as a leader in cyberspace as part of its recruiting strategy. The Air Force brand is one that dramatically sets the Air Force apart from the other armed services. The best work on understanding the public perception of the Air Force brand has been and continues to be done by the Joint Advertising and Marketing Research Studies (JAMRS) agency from the Department of Defense. JAMRS recent advertising tracking study indicated that of all the armed services, Air Force advertising is achieving the most success in

[17] American Marketing Association, ed., *Brand* (Chicago: American Marketing Association, 2014), accessed February 2, 2015, http://www.marketing-dictionary.org/ama. https://www.ama.org/resources/Pages/Dictionary.aspx?dLetter=B&dLetter=B.

reaching a technically oriented youth population. The most successful Air Force presentation in recent years, is the following:

> I wake up every day in the Air Force thinking I've got the best job in the world. Airplanes, jets, propeller planes, rockets, spaceships, starships. If it left the surface of the earth and went somewhere else on an adventure, it just captured my imagination. The opportunities that the Air Force can offer are boundless. When opportunity knocks at your door be bold, be courageous in following that dream, step across that threshold and into that new adventure. My name is Col. Alvin Drew and I am an American airman.[18]

JAMRS refers to the aforementioned advertisement as "Col Drew." The Col Drew advertisement is resoundingly successful on a number of levels. First, it is attracting more minorities and females to the Air Force than previous advertising campaigns. In particular JMARS found that that more females identify with the values and benefits of an Air Force career vice the other armed services. Second, the Col Drew advertisement reinforces the Air Force brand as being futuristic and forward thinking. JAMRS likewise conducted an investigation of perceived career values of the Air Force. The results provide an insight as to the public perception of the Air Force brand:

[18] "US Air Force Recruiter Online," US Air Force Recruiting Service, August 12, 2009, accessed October 22, 2014, http://www.rs.af.mil/recruiteronline/video/index.asp?cid=534&sid=24240.

Table 2. Air Force Perceived Career Values[19]

Perceived Career Value	Percentage of Respondents
Offers training in cutting-edge technology	52%
Is futuristic/forward-thinking	45%
Opportunities for unique job responsibilities	26%
Interesting and more than just a daily routine	23%
Make a good living	22%
Provides an opportunity for adventure	21%
Allows you to do great things with your life	21%
A lifestyle that is attractive to me	19%
Safe work environment	15%
Is with an elite organization	15%

Source: Cyber Security Census (Mechanicsville, VA: Semper Secure, 2013), 3.

The success of the Air Force in attracting the technically oriented people can be attributed, for the most part, in its ability to brand itself as the technical leader among the Army, Navy, and Marine Corps.

In contrast to the Air Force's focus on cyberspace at the start of the new millennium, private sector cyberspace capabilities has expanded at fervent pace since the early 1990's when the Internet began to be a more important part of our daily lives. Cyberspace growth in the private sector reached a new level in 2014 when General Motors named Jeffrey Massimilla as its first executive head of product cybersecurity.[20] The creation of this position was driven by congressional pressure on General Motors to protect digital automobile systems from hacking. Private sector experience in recruiting of cyberspace professionals precedes that of any of the armed services by at least a decade. This head start has allowed the private sector to develop and refine recruiting practices to achieve optimum success.

[19] *DoD Advertising Tracking Study: Overview of Wave 41 Results*, JAMRS (Washington, DC: Government Printing Office, 2013).

[20] Eduard Kovacs, "GM Appoints Chief Product Cybersecurity Officer," Security Week, September 24, 2014, accessed November 5, 2014, http://www.securityweek.com/gm-appoints-chief-product-cybersecurity-officer.

Although hiring only the best is a mantra used by almost any public or private sector organization, successful firms, such as Sprint, through organizational branding, have been able turn the mantra of hiring only the best into a reality. Sprint seeks to differentiate itself from competitors in terms of the technical challenges and opportunities that come with employment. Sprint's latest recruiting efforts appeal to their brand as a technical leader in cyberspace, "Pushing the frontier of what's possible. There is no limit to creativity, and at Sprint creativity and innovation are in our DNA. We are leaders in pioneering technologies and finding useful applications for those technologies."[21] Sprint branding allows it to successfully recruit the quality cyberspace workforce that allows it to be a leader in the marketplace.

In contrast to the Air Force and Sprint brands, the Army brand has been and continues to be one focused on values and service to the nation. To date this approach has been extremely successful for the Army. The ideal of service to the nation attracted many to the Army in the wake of the 9/11 attacks and the subsequent wars in Afghanistan and Iraq. The Army brand is broadcast through advertising campaigns developed and implemented by the Army. Commercials airing on television are the most effective and pervasive tool the Army uses to develop its brand. Evidence of the Army brand, the focus on values and service is plainly evident in the following commercial:

> There's strong and then there is Army strong. It is not just the strength to obey, but the strength to command. Not just strength in numbers, but strength of brothers. Not just the strength to lift, but the strength to raise. Not just the strength to get yourself over, but the strength to get over yourself. It is more than physical strength. It is emotional strength. There is nothing on this green earth stronger than the U.S. Army because there is nothing stronger on this green Earth than a U.S. Army Soldier. There's strong and then there is Army strong.[22]

---

[21] "Sprint Technology Careers," Sprint, 2014, accessed November 8, 2014, http://careers.sprint.com/technology.html.

[22] "US Army Recruiting Command," YouTube, August 9, 2013, accessed October 17,

However, in recruiting cyberspace professionals an Army brand based on values and service to the nation may not be the best approach to entice Generation Z to become the Cyber Mission Force Soldiers of *Force 2025 and Beyond*. The latest JAMRS study[23] provides the top career values associated with the Army:

Table 3. Army Perceived Career Values

Perceived Career Value	Percentage of Respondents
Allows you to serve as protector of your country	34%
Opportunity to become stronger	28%
Offers a strong sense of belonging	24%
Is something to be proud of	22%
Allows you to make a positive global impact	19%
Provides an opportunity for adventure	18%
Allows you to do great things with your life	18%
Opportunities for unique job responsibilities	16%
Make a good living	15%
Interesting and more than just a daily routine	15%

Source: DoD Advertising Tracking Study: Overview of Wave 41 Results, JAMRS (Washington, DC: Government Printing Office, 2013).

Accordingly, technically talented young men and women that are interested in pursuing a career in the armed forces will undoubtedly be drawn to the service that in their view is more technically oriented. One implication of the data as it relates to Army recruiting from the civilian population. The Army is not seen as futuristic or forward thinking. The work by Semper Secure shows that among those cyberspace professionals who did not switch careers, the primary motivator for a cyberspace career was technology.

2014, http://www.bing.com/videos/search?q=army+recruiting+videos&FORM=VIRE13#view=detail&mid=061FF579DAE09C510DE2061FF579DAE09C510DE2.

[23] *DoD Advertising Tracking Study: Overview of Wave 41 Results*, JAMRS, (Washington, DC: Government Printing Office, 2013).

The Air Force recruiting model takes personality and geographical characteristics into account. The Air Force understands that its future Cyberspace Airmen are not likely to be found on the athletic fields of the local high schools. The Air Force recognizes and capitalizes on the geographic nature of the cyberspace workforce. The Air Force targets its recruiting efforts heavily in the Seattle area which has a high density of information technology corporations. The product of the Air Force's Seattle focus is the 262nd Network Warfare Squadron. The 262nd Network Warfare Squadron is a National Guard unit that leverages a number of Airmen that hold traditional jobs with area firms like Microsoft. Sprint also realizes that a uniform approach to recruiting will not work when there is a small supply of potential candidates and a strong demand for those candidates. To attract the best and brightest of the digital natives into the Army, the Army must be able to target recruits using specialized recruiters with the skills of those being recruited. As the Army looks at its efforts, a one size fits all approach to recruiting will probably not succeed in filling the CyMF. Recruiters must also be able to coherently explain to those interested in joining the Army about the type of technical training and challenges that await them as part of the CyMF. This represents a departure from previous Army recruiting paradigms. Equally important as branding is the significance of compensation for those in technical careers.

High compensation for the most talented cyberspace professionals is one consequence of the low supply and high demand. The RAND Corporation in *H4cker5 Wanted*[24] developed a supply, demand, and compensation model for cyberspace professionals. The RAND model when combined with projected salary and compensation growth data can be used to project future conditions for entry level cyberspace professionals. Compensation for cyberspace professionals is

[24] Martin C. Libicki, David Senty, and Julia Pollak, *H4ckers5 Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, California: RAND, 2014), 42.

conservatively expected to grow annually by 8% for at least the next five years.[25] The RAND compensation model using projected salary data is graphically presented below.

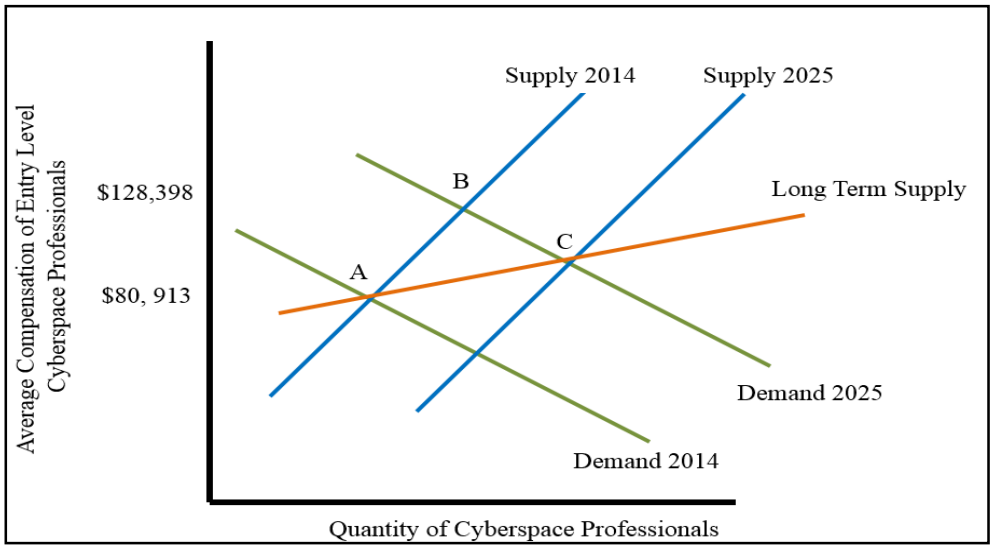

Figure 2. Cyberspace Career Compensation

Source: H4ckers5 Wanted: An Examination of the Cybersecurity Labor Market (Santa Monica, California: RAND, 2014), 42.

The compensation relationship, measured in Dollars, is $A < C < B$, where point *A* represents current average compensation of $80,913, point *B* represents the short term equilibrium of $128,398, and the point *C* represents the long term equilibrium. Projected compensation for entry level cyberspace professionals will peak at point *B* and then drop to point *C* once supply equals demand. The military, regardless of Service, cannot adjust to compensation differentials as quickly or easily as the private sector. The RAND model of compensation indicates that compensation for cyberspace professionals will be expected to increase for the next several years while schools work to meet public and private sector demand. However, once the demand is met

[25] Ann Bednarz, "2013 It Salaries," *NetworkWorld*, November 7, 2012, 1, accessed December 14, 2014, http://www.networkworld.com/article/2161278/infrastructure-management/2013-it-salaries--15-titles-getting-the-biggest-pay-raises.html

or if demand abates, it is expected that compensation levels across all cyberspace careers will decrease.

The previously cited Cyber Security Census considered two forms of compensation, intrinsic and extrinsic, that must be addressed as part of any successful recruiting strategy.[26] Intrinsic compensation consists of those quantifiable benefits one receives for work. This includes salary and benefits. Extrinsic compensation refers to the non-quantifiable benefits. For example, extrinsic compensation includes pride in the organization, corporate culture, and career development. Research by Tahir, et.al, 2011; showed conclusively that intrinsic compensation is valued above all other types of compensation by entry level employees.

Although many would dismiss compensation as a reason for joining the military, there are a large portion of eligible candidates that would join the military based on compensation. JAMRS research published in 2011 indicated that nearly 40% of civilian males surveyed indicated that economic conditions, such as difficulty in finding employment, would make military service a more likely option. At the same time, JAMRS discovered that 80% of those civilians surveyed, male & female, believe that military pay is not comparable to that in the private sector. JAMRS analysts believe the seemingly contradictory data can be attributed to the extremely high levels of civilian unemployment that remained following the recession of 2008. It is believed that the severity of unemployment at the time made military compensation attractive in spite of its perceived inadequacies.

The one commonality between the Air Force and the Army is basic compensation, at least in terms of intrinsic compensation. Military compensation is an amalgamation of several types of

[26] Ahmad Jamil Tahir, "A Comparison of Intrinsic and Extrinsic Compensation Instruments," *World Journal of Social Sciences* 1, no. 4 (September 2011): 195-206.

base pay, incentive pay, health benefits, education benefits, and vacation (leave). The entry level compensation for the Air Force and the Army was in 2014 is shown in the table below.

Table 4. Air Force and Army Entry Level Compensation[27]

Rank (USAF/Army)/Grade	Time in Service (Years)	Yearly/Compensation
Airman First Class / Private First Class / E3	2	$40,770.85
Senior Airman / Specialist / E4	4	$43,890.78
Staff Sergeant / Sergeant / E5	5	$45,179.58
N/A / Warrant Officer / WO1	8	$65,315.04
Second Lieutenant / Second Lieutenant / O1	1	$53,673.17
First Lieutenant / First Lieutenant / O2	3	$68,160.85
Captain / Captain / O3	4	$87,003.04

Source: Defense Finance and Accounting Service, "Military Compensation," Office of the Secretary of Defense, January 1, 2014

The one difference worth noting is that Air Force does not maintain a Warrant Officer rank structure whereas the Army does. While Table 4 provides a complete picture of intrinsic compensation, the intangible or extrinsic, value of military service, as documented in Table 4, is not included by its very nature. For instance, a military member pursuing a technical career would, based on perceived service values, have a larger extrinsic level of compensation serving in the Air Force rather than the Army.

Similarly, compensation packages for private sector cyberspace professionals cross both intrinsic and extrinsic forms. While military pay is set by Congress, private sector firms are free to set their own compensation levels. Highly successful firms, such as Sprint, can clearly offer higher levels of compensation than struggling firms in the industry. In order to determine private

[27] Defense Finance and Accounting Service, "Military Compensation," Office of the Secretary of Defense, January 1, 2014, accessed November 21, 2014, http://militarypay.defense.gov/mpcalcs/Calculators/RMC.aspx.

sector compensation industry averages were used. Average yearly compensation for entry level and mid-career professionals are found in the table below.

Table 5. Private Sector Compensation

Private Sector/Year		
Position	Entry Level	Mid-Career
Information Security Analyst[28]	$80,067	$129,560
Data Security Analyst[29]	$80,866	$132,681
Network Administrator[30]	$81,803	$116,913

Source: Salary.com, July, 2014.

Compensation in Table 5 includes salary, Social Security, 401K/403B, disability, health care, pension, and time off benefits. Some firms, such as Sprint, offer even larger compensation packages that include reduced rates for wireless services, wellness programs, adoption assistance, financial planning, and stock purchase plans. All of these additional benefits coupled with the extrinsic benefits of pride and elitism of working for a company like Sprint make the true value of compensation received much higher than that shown in Table 5.

Consequently, when compared to successful cyberspace recruiting approaches used by the Air Force and Sprint; the Army approach will likely fail based upon Army branding and compensation. Army messaging continues to focus on values and service to the nation as the impetus to join the Army. This messaging is in stark contrast to that of the Air Force. Recent data by JAMRS reflects this difference in perceptions between the two services.

[28] "Information Security Analyst," Salary.com, July, 2014, accessed July 24, 2014, http://swz.salary.com/salarywizard/Information-Security-Analyst-I-Salary-Details.aspx.

[29] "Data Security Analyst," Salary.com, July, 2014, accessed July 24, 2014, http://swz.salary.com/salarywizard/Data-Security-Analyst-I-Salary-Details.aspx.

[30] "Network Administrator," Salary.com, July, 2014, accessed July 24, 2014, http://swz.salary.com/salarywizard/Network-Administrator-I-Salary-Details.aspx.

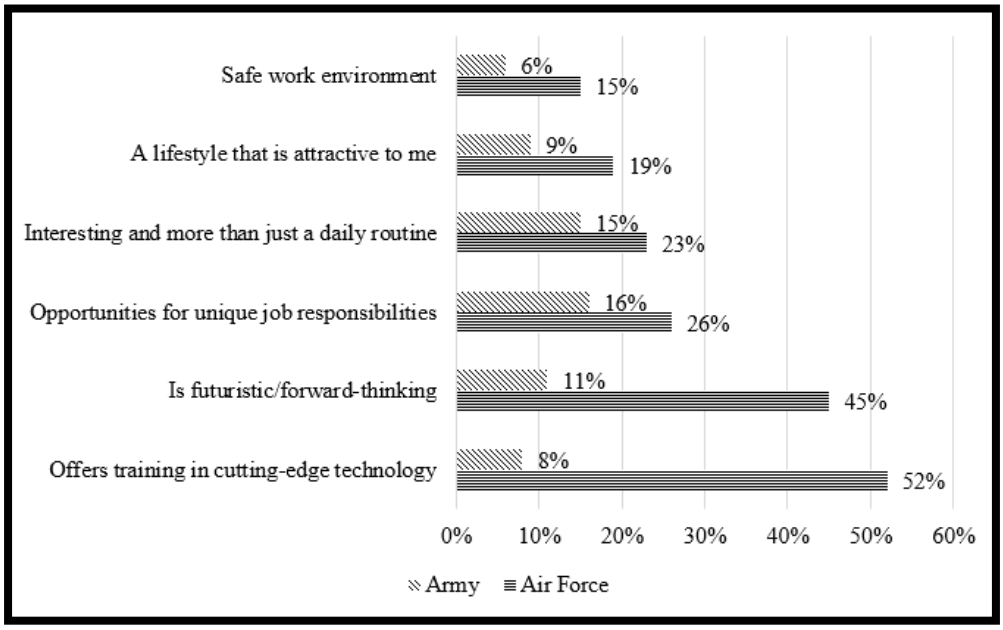

Figure 3 Army and Air Force Service Perceptions

Source: DoD Advertising Tracking Study: Overview of Wave 41 Results, JAMRS (Washington, DC: Government Printing Office, 2013).

The Army has chosen to pursue a one size fits all approach using values and service to cyberspace recruiting. While this approach is undoubtedly successful for recruiting infantrymen, artillerymen, logisticians, and others it will not, as shown previously, succeed for highly technical careers such as cyberspace. As shown earlier, aside from branding, the other key part of the recruiting problem is compensation.

In particular, by comparing Tables 3 and 5 it becomes clear that the Army will not be able to compete with private sector salaries for cyberspace professionals. The intrinsic compensation gap ranges are graphically shown below.

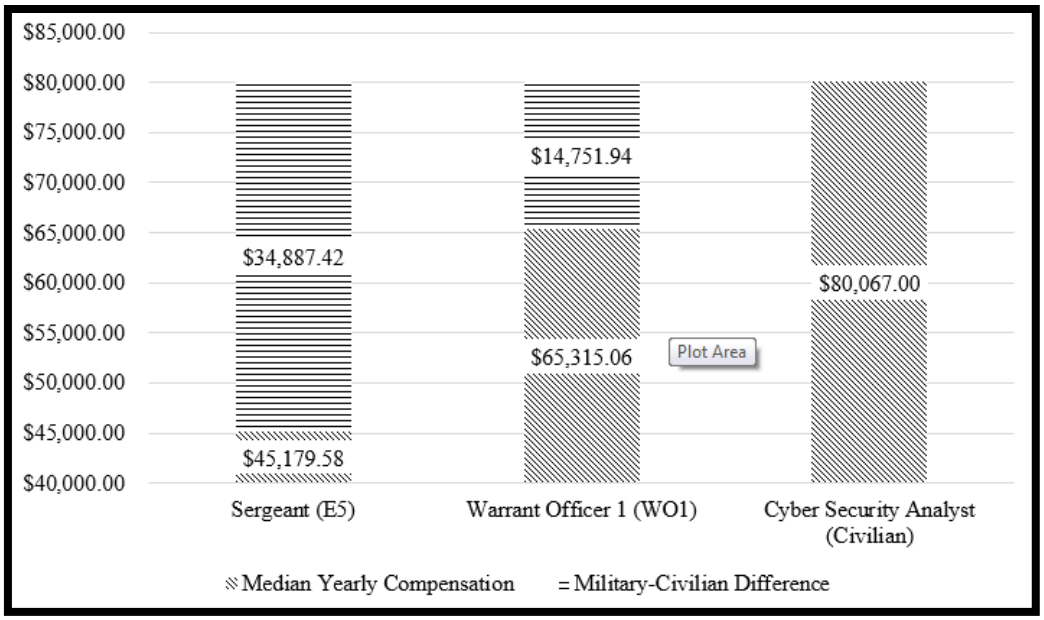

Figure 4 Army and Private Sector Compensation

Source: "Regular Military Compensation," Under Secretary of Defense, Personnel & Readiness, December 31, 2012.

Moreover, the Army cannot compete against the Air Force based on extrinsic compensation for entry level positions. The extrinsic benefits associated with service in the Air Force that are most applicable to this research include attractive lifestyle, safe work environment, interesting work, futuristic/forward thinking, cutting-edge technology, and unique job responsibilities. These six extrinsic benefits, most closely associated with the Air Force, are also the most prized by Generation Z and those drawn to technical careers. The focus on recruitment in the military, talent acquisition in the private sector, is but one part of the equation involved in developing a cyberspace workforce. The other part of the equation is retention for the military; talent management for the private sector.

Retaining the Best and Brightest

Retaining qualified, serving members of the armed forces is just as important as it is for the private sector since there are a number of shared concerns. A trained member of the military

represents a significant investment of time and money. The RAND Corporation estimated that the Army alone spends approximately $14,000 in recruiting costs for each new Soldier that comes into the Army. Add to recruiting cost the cost of Basic Training, approximately $50,000, leads to a total cost $64,000 per soldier. If the soldier enlisted in a technical field; e.g. Signal Corps, Military Intelligence, or Cyberspace, the additional training required could easily push the total amount invested in that one soldier to nearly $200,000. Retention is even more critical given the ability of cyberspace professionals to leave organizations with little concern about finding new employment. So while it is critical to discuss how to go about building a cyberspace workforce, whether military or private sector; it is equally critical to discuss how that workforce is maintained and managed. For the purpose of this work, retention will focus on compensation and career development using the Air Force and Sprint in comparison to the Army.

Currently, the US Air Force maintains the largest cyberspace workforce, both military and civilian, of all the armed services.[31] A key component of the Air Force success in maintaining its cyberspace workforce can be attributed to its use of bonuses, professional military education, and a career development model. It must also be noted among the armed services the Air Force had a big head start in developing a cyberspace workforce. As will be shown, the Air Force has already taken steps to streamline and manage its diverse cyberspace career fields better under a central management principle. The Air Force central management principle greatly facilitates the efficient management of its cyberspace workforce.

The Air Force employs a Selective Reenlistment Bonus, SRB, program to retain those Airmen in critical career fields such as cyberspace. A selective re-enlistment bonus is only available to Cyberspace Defense Operations Airmen. This is a very small career field of

[31] Oriana Pawlyk, "Cyber: The Safest Job in the Air Force," *Air Force Times*, February 20, 2014, 15.

approximately 500 Airmen, but growing. The Cyberspace Defense Operations Airmen are the most highly trained and are mission qualified for employing various cyberspace weapon systems. It is clear that the Air Force is significantly motivated to retain the Cyberspace Defense Operations Airmen in whom it has invested so much in terms of training and responsibility. The Air Force SRB for these airmen is based on their current pay rate and length of reenlistment. The general terms mandate that 50% of the SRB is paid up front, and the remainder is split equally across each year on the re-enlistment. The Air Force has specifically targeted mid-career Noncommissioned Officers with 6-10 years of service to receive the largest bonuses. For example, an E6 with eight years of service that re-enlists for an additional six years could qualify for $38,000 up front and then $6,500 per year for six years. This bonus would equate to a bonus of $77,000.[32] Moreover, the Air Force has focused on more than just compensation to maintain its cyberspace force. Additionally, airmen in cyberspace career fields are not subject to force reductions which makes these career fields especially attractive.

Although the basic pay tables in the Department of Defense is set by Congress, the services are given the freedom to determine promotion timelines which directly influence the amount of compensation a service member receives. The Air Force tends to have slower promotions, in other words longer time in service, than does the Army. The slower promotion rate means that an Air Force NCO in the same grade as an Army NCO receives a greater pay because he usually has longer time in service.

[32] Ibid. Short Citation Required

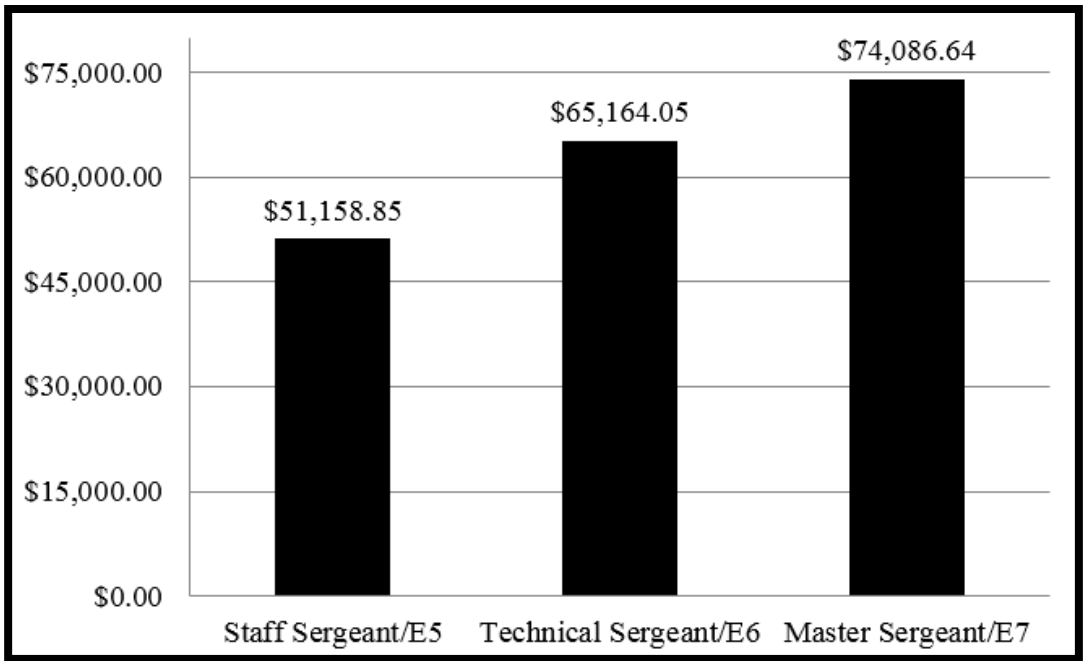

Figure 5 Air Force Mid-Career Compensation

Source: "Regular Military Compensation," Under Secretary of Defense, Personnel & Readiness, December 31, 2012.

In like fashion, the private sector also faces challenges in retaining trained cyberspace professionals. However, Sprint has achieved unparalleled levels of success in retaining its cyberspace workforce. ComputerWorld reported that Sprint achieved a 1.9% voluntary turnover rate which is one of the best in the industry.[33] Much like any other organization, public or private, Sprint realizes that compensation matters. In this regard, Sprint created a short-term incentive program that, "rewards eligible employees for exceptional business performance. As part of our total compensation package, employees have the opportunity to earn a percentage of base pay as a bonus for helping Sprint achieve its financial and customer service objectives."[34] The Sprint

[33] Mary Pratt, "Best Places Spotlight: Sprint Nextel," *Computerworld*, June 18, 2012, accessed March 25, 2015, http://www.computerworld.com/article/2504193/it-management/best-places-spotlight-sprint-nextel-keeps-it-pros-engaged.html.

[34] "Sprint Careers," Sprint, 2015, accessed March 25, 2015, http://careers.sprint.com/work.html.

approach of offering attractive compensation undoubtedly helped Sprint reach the 1.9% voluntary turnover rate mentioned earlier.

Analogous to the Air Force and Sprint approaches, the management of the size of the Army is one that requires constant analysis to determine its current and future needs. The Army has a number of compensation based tools available that allow it to manage force levels. To increase a Career Management Field, CMF, the Army uses the Selective Reenlistment Bonus (SRB), the Enhanced Selective Reenlistment Bonus (ESRB), the Deployed Selective Reenlistment Bonus (DSRB) along with the now rescinded Bonus Extension and Retraining Program (BEAR) to retain and grow strength in that particular field. Based on evolving force requirements the force management process, by its very nature, is one that is highly dynamic.

When the Army transitioned from the draft to the All-Volunteer Force one of the first programs initiated in June 1972 was the Enlistment Bonus. The current SRB programs; SRB, ESRB and DSRB; replaced the Enlistment Bonus, Regular Reenlistment Bonus, and the Variable Reenlistment Bonus in 1974. The SRB programs are designed to provide a bonus for the soldiers currently serving in critical MOSs that agree to reenlist for three years. The amount of the bonus paid to the soldier can be any one of the following: $45,000, six-times the monthly base pay at time of discharge, or $20,000. The now defunct BEAR program was one that sought to transfer soldiers from over strength MOSs into those MOSs deemed critical by the Army. The soldiers electing for the BEAR program received a bonus along with training in the new MOS. Research by the RAND Corporation in 2010 determined that for the Army, the opportunity to receive a bonus and promotion to a higher rank had the greatest impact on the decision to reenlist. RAND found a statistically significant correlation between the amount of the bonus and the propensity to reenlist. Another interesting fact discovered by the researchers was that Sergeants (E5) were more than 30% more likely to reenlist than Specialists (E4). Analysis attributed this

gap to the sergeants perceived future gains in rank, pay, and responsibility that accompany further service in the Army. Compensation based on promotion and time in service is the same across all of the Army Military Occupation Specialties. For the purposes of this work the focus will be on those Noncommissioned Officers that can be considered to be mid-career NCO's. Based on traditional career timelines the ranks identified are past their initial enlistment but are not past the point of being able to retire.

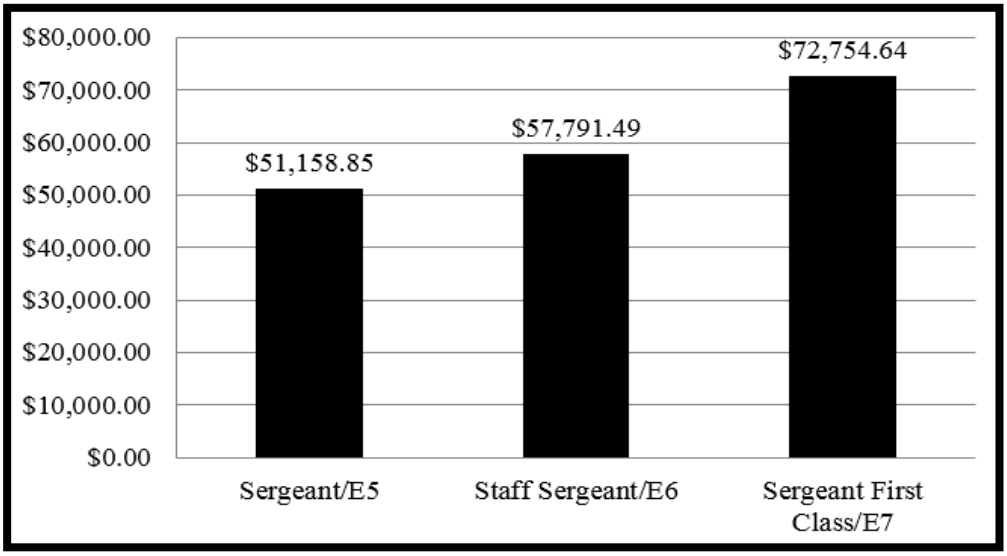

Figure 6 Army Mid-Career Compensation

Source: "Regular Military Compensation," Under Secretary of Defense, Personnel & Readiness, December 31, 2012.

Not represented are the various types of incentive pay that the Army offers to select individuals based up duty assignment, duty location, or specialized skill.

Compensation is critical in not only recruiting, but also in retaining cyberspace professionals. For this reason, the Army will likely fail to retain qualified cyberspace professionals because it does not approach the problem in a manner similar to the successful approaches used by the Air Force and Sprint. The Air Force and Sprint have each taken different approaches to offer competitive compensation to retain those with critical cyberspace skills. The Air Force approaches this problem using bonuses and different promotion timelines. In contrast,

Sprint Corporation ranks positions based upon criticality and compensates accordingly. The end result is that both the Air Force and Sprint use specific and targeted compensation programs to retain qualified cyberspace professionals. On the other hand, the Army has not chosen to target compensate cyberspace professionals. Title 37, Chapter 5, of the US Code covers special and incentive pay (S&IP) for Active Duty military members. An overwhelming majority of Title 37 covers S&IP for military members in the medical fields. The bulk of the remaining authorization allow S&IP for aviation fields and hazardous duty. For the interest of maintaining a CyMF, Army might use Section 355, Critical Skills Retention Bonus (CSRB), but it is an approach the Army has not pursued. Per the US Code, Section 355, provides the services a means to offer incentives to address key personnel shortages. For example, up to $200K total ($100K for reserve component members) is payable in CSRB to an eligible member over a career.[35] Employing a CSRB type of option brings the added benefit of encouraging the service member to stay for an entire career of 20 years in order to realize the full benefit. Rather, the Army has pursued a compensation construct that while effective for non-technical fields may not succeed for highly technical fields such as cyberspace.

Professional development, with compensation, also determines whether or not an organization will retain an employee. The most appropriate definition a professional development comes from the Training and Development Handbook: “the process by which individuals increase their understanding and knowledge, and/or improve their skills and abilities, to perform better in their current positions or to prepare themselves for a position to which they realistically aspire to in the

[35] “Special and Incentive Pay Index,” Under Secretary of Defense, Personnel & Readiness, December 31, 2013, accessed November 8, 2014, http://militarypay.defense.gov/PAY/SI/SIINDEX.ASPX#355.

near future."[36] Professional development supports retention through increased morale and job satisfaction.

As the armed service with the longest history in cyberspace, the Air Force has altered its professional development model to improve retention of critical cyberspace professionals. The Air Force has reduced the length of its Noncommissioned Officer schools significantly over the past several years. For example, the Air Force Senior Noncommissioned Officer Course is only 6.5 weeks long. The reduction in course length accompanied the addition of an online portion prior to resident attendance in the course. The benefit of shorter resident schooling in subjects that are not MOS specific means Air Force cyberspace professionals are not absent from their primary duties for long periods and hence, able to remain proficient in their technical skills.

The Air Force approach to cyberspace career development, as part of its larger professional development construct, is one that clearly exemplifies the service's technical skill paradigm as compared to the other armed services. The Air Force views enlisted career development through the guild like paradigm. Cyberspace airmen begin their careers as Apprentices (E2-E4), then become Journeymen (E5-E6), then Craftsmen (E7-E8), and finally Superintendents (E9). While the terms may seem quaint, they provide a greater insight into the model by which the Air Force designed their cyberspace career fields. Air Force career development for cyberspace airmen continually integrates technical education and training into the process. Throughout their careers an airman in a cyberspace field will attend the following technically oriented cyber training: Technical Training School, Upgrade Training, Cyberspace Craftsman Course, and Cyberspace Superintendent Course along with various professional

[36] Robert L. Craig, Training and Development Handbook: A Guide to Human Resource Development, 3rd ed. (New York: McGraw-Hill, 1987), 37.

certification courses. Additionally the Air Force provides opportunities for its more talented airmen to participate in broadening assignments that further build and refine their technical skills.

Likewise, Sprint approaches professional development in a manner very similar to that of the Air Force. Sprint's Chief Information Officer (CIO) Peter Campbell was asked in a 2012 interview what makes Sprint's most talented workers stay. Mr Campbell responded, "We provide them with the opportunity to do challenging work, with interesting technology. We also provide opportunities for training, job rotations and career advancement that our employees appreciate."[37] Sprint took professional development of its workforce to a higher level with the establishment of Sprint University (SU). Sprint University is focused on investing in its workforce by:

> supporting your performance and professional development . . . to provide you the right solution at the right time to support your on-going learning and skills development. With expertise in performance support, development, and delivery, the SU staff has the knowledge and hands-on experience to help you reach your full potential through innovative and engaging solutions.[38]

Sprint's focus and commitment to professional development ensures a workforce that is committed to the corporation.

Nonetheless, the Army development model of education, training, and experience is one that has served it well over the past several decades. The model allows for increasing responsibility and authority, while exposing the soldier to a wide variety of assignments, geographic locations, and professional military education (PME). An Army soldier transitions from technical duties to more leadership intensive roles and responsibilities. With the increase in rank the soldier receives increases in compensation, primarily salary based on rank and time in

[37] *Computerworld*, Premier 100 IT Leaders, 2012, accessed March 25, 2015, http://www.computerworld.com/premier100/detail/411.

[38] "Sprint Careers," Sprint, 2015, accessed March 25, 2015, http://careers.sprint.com/work.html.

service. In the end, a successful soldier will complete their career and retire after 20 years at the rank of Sergeant First Class or higher. The focus of this work will be to analyze those factors that have been shown to be the most influential in retaining a Soldier in the Army. The factors that will be investigated include: bonuses, education, compensation, and duty responsibilities.

The Noncommissioned Officer Education System (NCOES) is the foundation of the Army's professional Noncommissioned Officer Corps. The NCOES begins at the Warrior Leader Course, continues to the Advanced Leader Course, then to the Senior Leader Course, and culminates at the Sergeants Major Course. These courses, all resident at various locations, vary in length from several weeks to several months and focus primarily on turning noncommissioned officers into the leaders that the Army needs. It is hoped that through investing in the professional development of an NCO, through NCOES, the Army will retain the soldier.

The Army's professional development model grows and challenges soldiers through assignments to positions with increasing responsibility. As the noncommissioned officer becomes more senior, the lifecycle development model provides that NCO with wider and more diverse leadership positions such as Platoon Sergeant, First Sergeant, and Command Sergeant Major. As the NCO focuses more on traditional Army leadership positions, the percentage of his technical responsibilities drops significantly. The current lifecycle development model does not take into account the possibility that an NCO would rather stay technically focused.

The comparisons of professional development strategies is another indication that the Army's approach to developing a CyMF will likely not succeed. The Air Force realized that technical professionals want to stay technically focused throughout their careers. The Air Force professional development model allows for technically focused career. Like the Air Force, Sprint allows an employee to stay at the same position or geographic location throughout their entire career. Sprint realizes that the institutional expertise and knowledge developed through this

approach is indispensable. It also takes into account that there will always be a small number of employees that want to switch positions and locations throughout a career. In contrast, Army retention for cyberspace professionals rests upon a professional development model that moves the NCO from technical duties to management responsibilities. Upon entering the Army the Cyberspace Specialist will find his duties entirely technical. Over time the duties will transition from technical to more managerial. The net result is that the technical specialist is transformed into a leader andmanager. This concept fits the common needs of the Army. However, members of Generation Z and those drawn to highly technical fields, such as cyberspace, want to remain technically focused. The intent of the Army model is to create a generalist based on wide variety of assignments. The unintended consequence, that is even more significant for cyberspace professionals, is that it does not allow the soldier to become an expert in their field.

Organized for Success

How the force is organized impacts both recruitment and retention. The importance of organization is best stated by employee training specialist Robert L. Craig, "While effective organization of efforts requires considerable research and analysis, it is the key . . . because it provides the systematic means to coordinate related resources so that specific objectives can be reached efficiently and effectively."[39] The key point of Craig's quote is that successful organizations are those that are structured for resource efficiency and effectiveness.

Based upon nearly a decade of experience, the Air Force re-organized its cyberspace structure in November 2009. It established a ***single*** Air Force Specialty Code (AFSC) 3D, Cyberspace Operations. The AFSC 3D construct consolidated AFSC 2E, Communications-

[39] Robert L. Craig, *Training and Development Handbook: A Guide to Human Resource Development*, 3rd ed. (New York: McGraw-Hill, 1987), 26.

Electronics Systems; AFSC 3A, Information Management; and AFSC 3C, Communications-Computer Support. Those career fields consolidated under AFSC 3D include:

- 3D0X1, Knowledge Operations Management
- 3D0X2, Cyber Systems Operations
- 3D0X3, Cyber Surety
- 3D0X4, Computer Systems Programming
- 3D1X1, Client Systems
- 3D1X2, Cyber Transport
- 3D1X3, RF Transmission Systems
- 3D1X4, Spectrum Operations
- 3D1X5, Radar
- 3D1X6, Airfield Systems
- 3D1X7, Cable and Antenna Systems

Referring back to Robert Craig's quote in the beginning of this section, the Air Force organization for cyberspace career fields improves efficiency and effectiveness by providing for unity of command and centralized management and training for all Air Force cyberspace professionals.

In a similar manner, Sprint organizes itself in a manner similar to the Air Force model. At Sprint all cyberspace specialties are trained and managed by one person,Chief Information Officer Peter Campbell and his staff. This single approach allows Sprint to achieve better talent acquisition and more importantly talent management. It allows Mr. Campbell and his team to grow and develop the workforce as they see industry trends evolving. More importantly senior executives at Sprint can identify and cultivate talent.

In late 2014, the Cyber Center of Excellence formalized the Army approach to the larger organizational problem for establishing the CyMF. Following a nearly month long working group in August 2014 the proposal was made to establish a Career Field 17 (CF17). CF17 is a new career field focused on leading, planning, and executing OCO and DCO within CyMF teams and their respective commands. CF17 consists of MOS 17A, Cyber Operations Officer for

Commissioned Officers; MOS 170A, Cyber Operations Technician for Warrant Officers; and MOS 17C, Cyber Operations Specialist for Enlisted Soldiers. Unique CF17 functions include:[40]

1. Executing, leading, and planning OCO and DCO mission through cyberspace Intelligence, Surveillance, & Reconnaissance (ISR), Operational Preparation of the Environment (OPE); attack and defend actions.
2. Creation of cyber effects (degrade, disrupt, destroy, manipulate) against adversaries and ensure friendly freedom of maneuver through cyberspace.
3. Integration of the Warfighting Functions into Cyberspace Operations.

Ultimately the CF17 represents a corps of Army soldiers fully capable of succeeding in any variety of Army and Joint cyberspace specific assignments. CF17 soldiers will form the foundation of the CyMF and the Cyber Protection Brigade.

The Cyber Protection Brigade (CPB) represents the Army's first effort to institutionalize a cyberspace capability in the force. The CPB, based at the Cyber Center of Excellence, consists of a headquarters with 20 subordinate Cyber Protection Teams. Each Cyber Protection Team consists of 39 Soldiers with a diverse array of cyber related skills. Key tasks for the CPB/CPT include: mission protection, discovery & counter-cyber, cyber threat emulation, compliance & operational readiness, and general technical support.[41] The 20 Cyber Protection Teams require a total of 780 trained Soldiers. The 20 Army Cyber Protection Teams are part of the 116 Cyber Teams that the Department of Defense expects to fill by 2016.

Rather than developing a single unified career structure, the Army has essentially developed three separate structures for cyberspace in the force. The Army's Signal and Military Intelligence Corps will each retain cyberspace capabilities and organizations with the associated personnel needed to provide these capabilities. In addition to the cyberspace capabilities provided

40. US Army Cyber Center of Excellence, *Career Field 17 Development Panel Outbrief* (Washington, DC: US Government Printing Office, 2014), 4.

41. 7th Signal Command, *Cyber Protection Brigade Recruiting* (Washington, DC: US Government Printing Office, 2014).

by the Signal and Military Intelligence Corps the addition of the new cyberspace career field, CF17, now introduces a new variable into an already complex problem. The structure chosen by the Army has many unintended consequences, most significantly in the area of recruiting of cyberspace professionals. As shown, the supply of those suitable to become cyberspace professionals, whether it is in the armed services or in the private sector is and will continue to be well below demand. The competition for these future cyberspace professionals will be intense. The Army has unintentionally created internal competition between the Signal Corps, Military Intelligence Corps, and the Cyberspace Career Field. This internal Army competition could very well prove disastrous to the Army goals for cyberspace. The Army has in actuality created three separate cyberspace workforces each with different training programs and professional development paradigms. The Signal Corps, Military Intelligence Corps, and Cyberspace Career Field will each develop and resource programs to train their respective cyberspace workforce.

Two examples of the separate cyberspace specialties within the Signal and Military Intelligence Corps illuminate the redundancies. Within the Signal Corps there is a Military Occupation Specialty (MOS) 25D – Cyber Network Defender. The cyber network defender's major duties include protecting, monitoring, detecting, analyzing, and responding to unauthorized cyberspace domain actions; and deployment and administration of computer network defense infrastructures, such as firewalls, intrusion detection systems and more.[42] Similarly, the Military Intelligence Corps has an MOS 35Q, Cryptologic Network Warfare Specialist. He is responsible for performing cryptologic digital analysis to establish target identification and operational patterns. The 35Q identifies, reports, and maintains intelligence information, analyzes

[42] "Cyber Network Defender (25D)," accessed January 20, 2015, http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-network-defender.html.

information, and prepares technical products and reports in support of Cryptologic Network Warfare operations."[43] These are but two examples, by no means a complete listing, of cyberspace specialties that fall outside of CF17.

Organizational structure analysis shows that the Air Force and Sprint approach are more effective and efficient. When the Army approach of separate career fields and organizations is similarly analyzed the results are not promising. The Air Force took a revolutionary step in organizing its entire cyberspace workforce under a single career field. This decision by the Air Force established unity of effort for recruiting and retaining cyberspace professionals. Even more important, Air Force created a common training foundation across its entire cyberspace workforce. Sprint Corporation in a similar manner has organized its entire technical workforce under the direction of its Chief Information Officer. Much like the Air Force this single structure has allowed Sprint to achieve efficiencies that otherwise would not have been possible. The organizational construct is the one area where the Army differs most from the Air Force and Sprint. Some could wrongly attribute this difference to the very basic differences between the Army, Air Force, and Sprint. However comforting as this may seem it is not supported by the very similar functions that cyberspace professionals perform in the military and private sector.

[43] "Cryptologic Network Warfare Specialist (35Q)," US Army Recruiting Command, accessed January 20, 2015, http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/intelligence-and-combat-support/cryptologic-network-warfare-specialist.html.

Conclusions

The new world of cyberspace in which the Army finds itself operating was best described by Lieutenant General Mark Bowman, J-6 of the Joint Staff, “the cyber enemy is an enemy that's potentially more dangerous than any individual or machine than we have ever known in the history of the world. We've got to be able to defend against the threat." For the Army to successfully maneuver in cyberspace means recruiting, retaining, and organizing the best possible CyMF. The current Army approach to developing a CyMF is likely to fail because it does not adequately address the unique challenges of recruiting, retaining, and organizing a highly technical workforce.

First, Army recruiting strategies are flawed because they do not address two primary factors, branding and compensation. Army branding, based upon values and service, will continue to be a major hurdle for the Army as it builds the CyMF. The perception among eligible recruits, as shown by JAMRS, is that the Army does not offer the technical skills or technical experience. This view will continue to drive technically qualified candidates into the other armed services, most notably the Air Force. Empirical studies presented in this work clearly show that the high demand-low supply of cyberspace professionals has created job market in which the most talented are drawn to those organizations providing the highest compensation. While the Army does offer attractive benefits, it does not, compete with the compensation, including bonuses, offered by the Air Force, or the private sector.

Second, in addition to the difficulties with the Army recruiting model, there exist significant problems with the Army approach to CyMF retention. The Army retention paradigm suffers from two major problems,compensation and professional development. As mentioned previously, compensation is vital in recruiting but equally so in talent retention. Army compensation has not taken into account the gap that exists between Army and private sector mid-career cyberspace professionals. Additionally, the Army development model transforms

technical specialists into leaders and managers. However, cyberspace professional prefer to become technical expects and avoid managerial responsibities. As shown in this work, there is an overwhelming desire for cyberspace professionals to remain technically focused throughout their professional careers. The Army model runs counter to this desire and, thus, will ultimately lead to retention difficulties.

Finally, the Army has made a serious misstep in the way it has organized for cyberspace. Rather than merge all cyberspace career fields under a single management construct, the Army has instead dispersed cyberspace capabilities within the Signal Corps, Military Intelligence Corps, and the newly formed Career Field 17. This Army decision created three different career fields with strikingly similar capabilities and responsibilities. This decision to maintain three separate cyberspace career fields inadvertently creates internal Army competition for the limited number of qualified soldiers and potential soldiers.

Based on recent events, there is no reason to believe that Army forces will not be subject to cyberspace attack. Potential adversaries have developed or are developing cyberspace warfare capabilities specifically aimed at countering US technological superiority. Former USCYBERCOM Commander, General Keith Alexander told Congress in February 2014 that military mission command systems, communication systems, and logistical support systems are especially vulnerable to cyberspace attack. The growing number of cyberspace actors and threats pose a significant challenge to the Army. This challenge will be greatly compounded if the Army is faced to confront these challenges shorthanded.The Army may face these cyber-threats shorthanded if it does not depart from standard Army personal practices and address the special charactistics of the very technical cyberprofessional.

Bibliography

7th Signal Command. Cyber Protection Brigade Recruiting Brief. Washington, DC: US Government Printing Office, 2014.

American Marketing Association. "Marketing Resource Dictionary." American Marketing Association. 2014, accessed February 2, 2015, http://www.marketing-dictionary.org/ama.

Bednarz, Ann. "2013 IT Salaries." NetworkWorld. November 7, 2012, accessed December 14, 2014, http://www.networkworld.com/article/2161278/infrastructure-management/2013-it-salaries--15-titles-getting-the-biggest-pay-raises.html.

Computerworld. Premier 100 It Leaders. 2012. Accessed March 25, 2015. http://www.computerworld.com/premier100/detail/411.

Craig, Robert L. *Training and Development Handbook: A Guide to Human Resource Development*. 3rd ed. New York: McGraw-Hill, 1987.

Csorny, Lauren. "Careers in the Growing Field of Information Technology." US Bureau of Labor Statistics. April 2013, accessed November 10, 2014, http://www.bls.gov/opub/btn/volume-2/careers-in-growing-field-of-information-technology-services.htm.

Finckle, Jim and Randewich, Noel. "Experts Warn of Shortage of U.S. Cyber Pros." Reuters. June 12, 2012. http://www.reuters.com/article/2012/06/12/us-media-tech-summit-symantec-idUSBRE85B1E220120612.

Information Security Analyst. July 2014. http://swz.salary.com/salarywizard/Information-Security-Analyst-I-Salary-Details.aspx.

Ivanovic, A. *Dictionary of Human Resources and Personnel Management*. 2nd ed. Teddington, Middlesex: Peter Collin Publishers, 1997.

Joint Advertising and Marketing Research Studies (JAMRS). DOD Advertising Tracking Study: Overview of Wave 41 Results. Washington, DC: Government Printing Office, 2013.

Kovacs, Eduard. "GM Appoints Chief Product Cybersecurity Officer." Security Week. September 24, 2014. http://www.securityweek.com/gm-appoints-chief-product-cybersecurity-officer.

Libicki, Martin C., David Senty, and Julia Pollak. *H4ckers5 Wanted: An Examination of the Cybersecurity Labor Market*. Santa Monica, California: RAND, 2014.

Lishia Whitworth and Sara White. "Facts About Gen Z." Tech with Class. August 20, 2014. Lishia Whitworth and Sara White, “Facts About Gen Z,” Tech with Class, accessed August 20, 2014, http://techwithclass.webs.com/facts-about-gen-z.

Pines, Susan, Veda Dickerson, and Lori Cates. "Experience." In O*NET Dictionary of Occupational Titles, 15. Indianapolis: JIST Publishing, 2003.

Pratt, Mary. “Best Places Spotlight: Sprint Nextel.” Computerworld, June 18, 2012. Accessed March 25, 2015. http://www.computerworld.com/article/2504193/it-management/best-places-spotlight-sprint-nextel-keeps-it-pros-engaged.html.

Semper Secure. Cyber Security Census. Mechanicsville, VA: Semper Secure, 2013.

Sprint Corporation. Sprint Technology Careers. 2014. http://careers.sprint.com/technology.html.

Tahir, Ahmad Jamil. "A Comparison of Intrinsic and Extrinsic Compensation Instruments." World Journal of Social Sciences, 2011: 195-206.

Thompson, Mark. "Panetta Sounds Alarm on Cyber War Threat." Time. 10 12, 2012. https://nation.time.com/2012/10/12/panetta-sounds-alarm-on-cyber-war-threat/.

US Air Force Recruiting Service. Recruiter Online. August 12, 2009.

US Army Cyber Center of Excellence. Career Field 17 Development Panel Outbrief. Washington, DC: US Government Printing Office, 2014.

US Army Recruiting Command. Army Recruiting Videos. August 9, 2013. http://www.bing.com/videos/search?q=army+recruiting+videos&FORM=VIRE13#view=detail&mid=061FF579DAE09C510DE2061FF579DAE09C510DE2.

Under Secretary of Defense, Personnel & Readiness. Military Compensation. January 1, 2014. http://militarypay.defense.gov/mpcalcs/Calculators/RMC.aspx.

US Army. Field Manual 3-38, *Cyber-Electromagnetic Activities*. Washington, DC: US Government Printing Office, 2014.

US Bureau of Labor Statistics,. "Information Security Analysts." U.S. Bureau of Labor Statistics. January 8, 2014. U.S. Bureau of Labor Statistics, “Information Security Analysts,” U.S. Bureau of Labor Statistics, January 8, 2014, accessed August 14, 2014, http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.